www.sharelock.ai | info@sharelock.ai

Sharelock

The Convergence Revolution

How Identity Security Finally Bridged the SecOps-IT Divide

For decades, cybersecurity has suffered from a fundamental architectural flaw: the artificial separation between identity management and security operations. While IT departments managed identities in isolation and Security Operations Centers (SOCs) monitored threats in their own silo, attackers never respected these organizational boundaries. They exploited the gap between these domains with devastating efficiency, turning our internal divisions into their strategic advantage.

This fragmentation wasn't just an operational inconvenience—it was a critical vulnerability. And now, after years of mounting breaches and billions in losses, the industry is finally acknowledging what should have been obvious from the start: **identity and security must converge.**

The Historical Problem

Silos That Never Made Sense

The traditional enterprise security model relegated identity and access management (IAM) to IT operations, treating it primarily as a provisioning and lifecycle management function. Meanwhile, security teams focused on perimeter defense, endpoint detection, and threat hunting—often with limited visibility into identity-related risks. This separation created dangerous blind spots.

Consider the attacker's perspective: when threat actors breach an organization, they don't distinguish between "IT problems" and "security problems". They steal credentials, escalate privileges, move laterally through systems, and exfiltrate data—all while exploiting the fact that no single team has complete visibility into the identity layer. According to recent data, valid accounts and compromised credentials represent 30-31% of initial access vectors in 2024, yet these attacks often went undetected because identity systems weren't being monitored with the same rigor as endpoints or networks.

The disconnect was absurd: **identity became the new perimeter,** yet it remained managed by teams whose primary focus was provisioning efficiency rather than threat detection. IT managed who could access what, but security teams were the ones responding when those identities were compromised. The lack of integration meant that by the time SOC analysts detected anomalous behavior, the attacker had already been moving laterally for days or weeks.

Gartner's Wake-Up Call

The Birth of ITDR

In 2022, Gartner analysts crystallized this problem by introducing a new category: **Identity Threat Detection and Response (ITDR)**. The firm listed it among their top security and risk management trends, explicitly acknowledging that traditional IAM hygiene practices—privileged access management (PAM) and identity governance—were no longer sufficient.

Gartner's rationale was stark: sophisticated threat actors were now directly targeting identity and access management infrastructure, and credential misuse had become "a primary threat attack vector". The industry needed solutions that could not only manage identity posture but also **detect and respond to identity-based attacks in real time.**

However, I would argue that Gartner's framing, while necessary, was incomplete. ITDR addressed the detection and response gap, but it still treated identity as primarily a reactive security concern. What was missing was the acknowledgment that **identity security isn't just about catching bad actors—it's about proactive posture management, attack surface reduction, and hygiene enforcement.**

Identity: The First Attack Vector

The data is unequivocal. Multiple 2024-2025 reports confirm that **identity-based attacks have become the dominant initial access vector:**

30%
Valid accounts tied with exploiting public-facing applications at **30% of all incidents** in IBM X-Force engagements

71%
Compromised credentials showed a **71% year-over-year increase** according to IBM's 2024 breach report

31.4%
31.4% of incidents in 2024 involved valid accounts as the initial vector, up significantly from 2023

165
The Snowflake breach alone impacted **165 organizations** through stolen credentials lacking MFA, affecting hundreds of millions of customers

Yet despite this overwhelming evidence, many organizations continue to treat identity security as an afterthought—a compliance checkbox rather than a frontline defense. This is partly because **the responsibility for identity security remained fragmented**: IT owned provisioning, security

owned detection, and no one owned the convergence between them.

Beyond Detection

Identity Security Posture Management

Here's where the industry narrative often gets it wrong: **identity security is not just about threat detection and response**. Yes, catching compromised credentials and anomalous behavior is critical. But equally important—and often overlooked—is the proactive work of **Identity Security Posture Management (ISPM).**

ISPM addresses the "hygiene" problem that ITDR alone cannot solve:

- **Discovering and remediating orphaned, dormant, and ghost accounts** that create unnecessary attack surface
- **Enforcing least privilege** by identifying and removing excessive permissions
- **Monitoring MFA adoption and policy deviations** across identity platforms
- **Detecting misconfigurations** before they can be exploited

The critical insight—one that took the industry too long to grasp—is that **ISPM and ITDR are two sides of the same coin**. You cannot have effective identity security by focusing solely on real-time threat detection while ignoring the toxic combinations of permissions, stale accounts, and policy violations that create vulnerabilities in the first place. Conversely, perfect identity hygiene means little if you cannot detect when an attacker compromises a legitimate account and begins moving laterally.

This is why the convergence between ISPM and ITDR represents a fundamental architectural shift, not just a product category consolidation.

The CyberArk-Palo Alto Deal

Convergence Goes Mainstream

For years, forward-thinking vendors and analysts understood the need for this convergence, but the market moved slowly. Then, in **July 2025, Palo**

Alto Networks announced its $25 billion acquisition of CyberArk, the largest identity security deal in history and the third-largest cybersecurity M&A ever.

Palo Alto was explicit about its rationale:

1. **The convergence of identity and security** as a market inflection point
2. **The need for platformization** in identity security
3. **The rise of machine identities and AI agents** requiring unified controls

As Forrester analyst Allie Mellen noted, this deal signaled Palo Alto's "mission to become a huge platform player", with identity security being "the missing piece of that puzzle". The acquisition made clear that the era of standalone, siloed identity solutions was ending. The future belonged to **integrated platforms that bridge network security, cloud security, endpoint protection, and identity security** under unified visibility and control.

Critics rightly point out that mega-acquisitions like this carry integration risks. The CyberArk user base—focused on privileged access management and identity protection—operates with different priorities than Palo Alto's SOC-focused customers. Merging these worlds is complex. But the strategic direction is clear: **the industry is finally acknowledging that security and identity must operate as a unified system**, not isolated domains.

The CyberArk acquisition made convergence fashionable. But some organizations had already been building toward this vision for years.

Sharelock

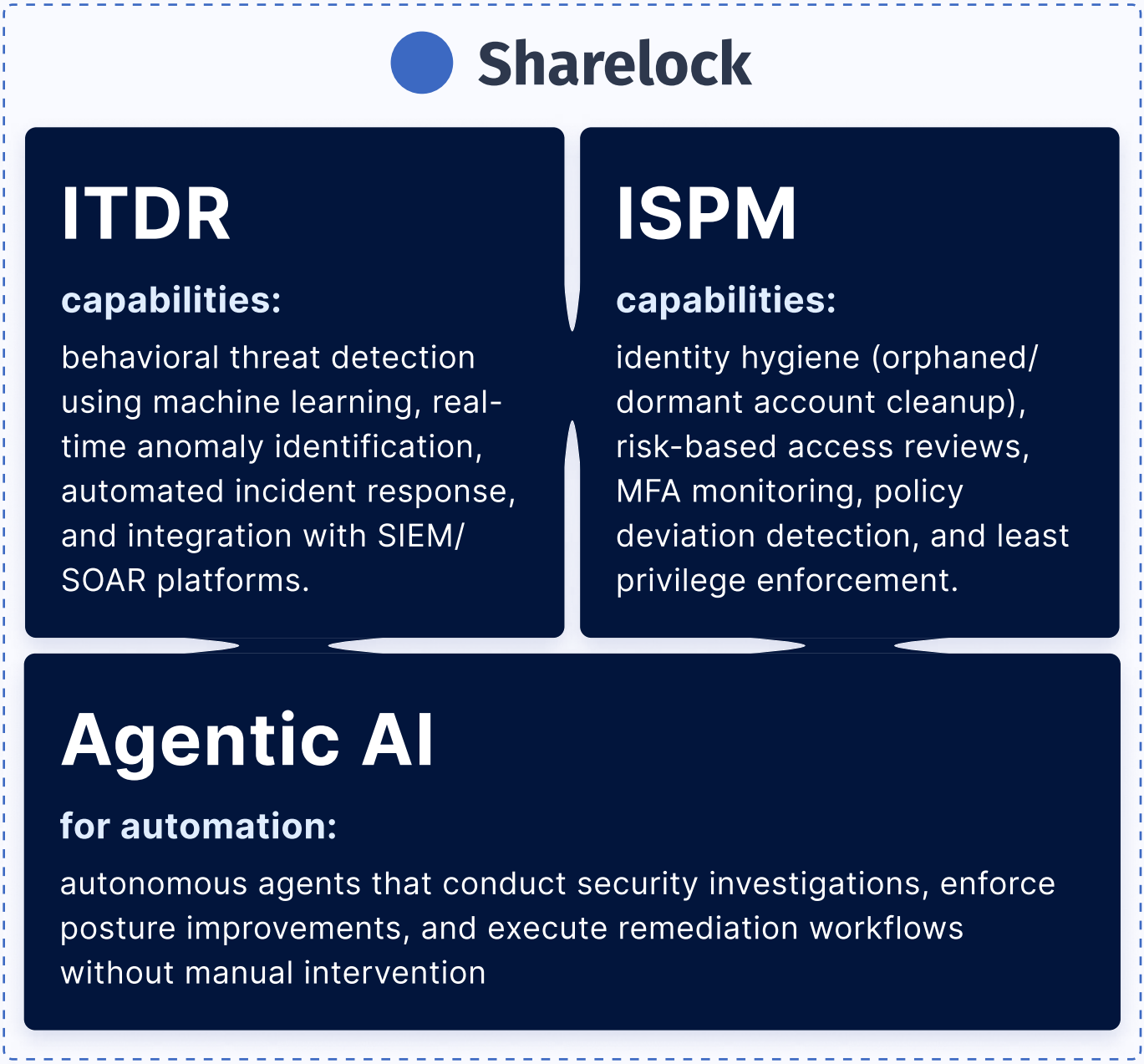
The Convergence Pioneer

While the market debated whether ISPM and ITDR should be separate categories, **Sharelock was already delivering both capabilities within a single, unified platform.** And its founding story embodies the very convergence thesis at the heart of this discussion.

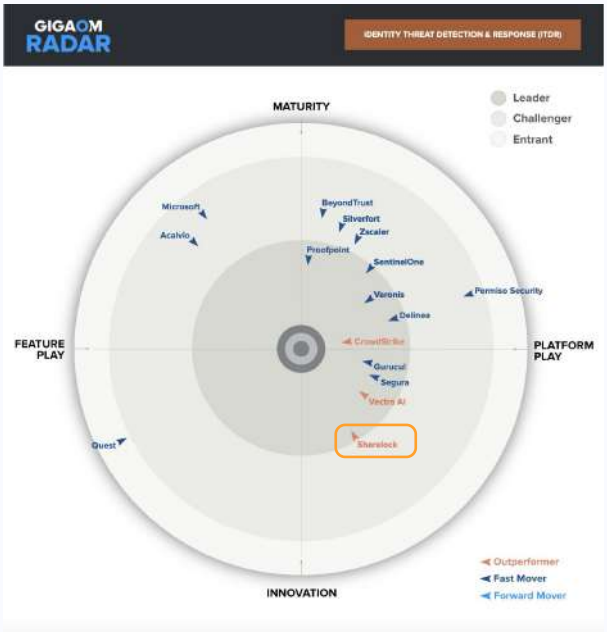
Sharelock's leadership came from **CrossIdeas, an Italian identity governance and administration company** that IBM acquired in **2014** to expand its Identity and Access Management portfolio. CrossIdeas specialized in access governance, role analytics, compliance, and risk management—the classic IAM domain. Its founders understood identity deeply, but they also saw the writing on the wall: **managing identity without monitoring threats was an incomplete solution.**

So they founded Sharelock with a radical premise: **identity security cannot be done in silos**.

The platform they built natively combines:



Sharelock predicted the convergence that the Palo Alto-CyberArk deal validated. By coming from the IAM world (CrossIdeas) and moving decisively into SecOps, the company shattered the artificial boundary that had plagued the industry for decades.



The results speak for themselves. In the **2025 GigaOm Radar for ITDR**, Sharelock is positioned as a **Leader and Outperformer in the Innovation/ Platform Play quadrant.** It's one of only two vendors (alongside CrowdStrike) designated as "Outperformer," recognizing its "continued rapid development" and "strong roadmap" driven by AI innovation. In the forthcoming **GigaOm Radar for ISPM**, Sharelock again appears as a **Leader**, further cementing its unique positioning as the **only platform that excels in both ISPM and ITDR domains.**

Moreover, Sharelock is featured in the **Gartner Emerging Tech report on Agentic AI integration in TDIR (Threat Detection and Response)**, alongside giants like CrowdStrike, Palo Alto Networks, and Vectra AI. This recognition underscores Sharelock's pioneering work in **autonomous AI-driven security operations and posture enforcement**—a capability that represents the future of identity security.

The European Advantage

Strategic and Geopolitical Importance

There's another dimension to this story that cannot be ignored: **Sharelock is the only European company delivering converged ISPM/ITDR capabilities at this level.** In an era where **digital sovereignty has become a top strategic priority** for the European Union, this matters profoundly.

Europe is increasingly focused on reducing dependence on non-EU technology providers, particularly in critical cybersecurity domains. Regulations like **NIS2, the Digital Operational Resilience Act (DORA), the**

Cyber Resilience Act, and the EU Cybersecurity Strategy all emphasize the need for European technological autonomy.

Consider the context:

> **96% of attacks from a highly influential pro-Russian hacktivist group targeted Europe** in 2024

> European critical infrastructure—hospitals, ports, energy grids—faces increasingly sophisticated attacks

> The EU is under pressure to build "resilient and trusted supply chains" for cybersecurity solutions, reducing reliance on vendors subject to extraterritorial legislation (such as the US CLOUD Act)

In this environment, **having a European-based, EU-sovereign identity security platform is not just a commercial differentiator—it's a strategic imperative.** For government agencies, defense organizations, critical infrastructure operators, and enterprises in regulated industries, the ability to deploy identity security without routing data through non-EU jurisdictions or depending on vendors subject to foreign government demands provides crucial independence.

Sharelock's positioning as a European champion in identity security aligns perfectly with these geopolitical realities. It offers institutional buyers, military organizations, and privacy-conscious enterprises a credible alternative that doesn't compromise on technology while meeting sovereignty requirements.

The Path Forward

Unified Identity Security as Standard

The convergence of identity management and security operations is no longer a visionary idea—**it's becoming table stakes.** The Palo Alto-CyberArk deal proves that the market has caught up to what pioneers like Sharelock have been building for years.

But let's be clear about what this convergence actually requires:

1. **Unified visibility:** a single platform that ingests identity telemetry from IAM systems, behavioral data from applications, and threat intelligence from security tools.
2. **Real-time detection and response:** behavioral analytics that can identify anomalies and automatically enforce remediation—blocking accounts, terminating sessions, triggering recertifications.
3. **Proactive posture management:** continuous hygiene enforcement that discovers misconfigurations, remediates excessive permissions, and reduces attack surface before threats materialize.
4. **Automation at scale:** Agentic AI that can autonomously investigate alerts, correlate multi-signal threats, and execute response playbooks without overwhelming security teams .

Organizations that continue to treat identity as an IT function separate from security operations are living in the past. **Attackers will continue to exploit that gap.** The question isn't whether to converge identity and security—**it's how quickly you can make it happen.**

The era of siloed identity security is over. The future belongs to platforms that unite posture management, threat detection, and automated enforcement—bridging the divide that should never have existed in the first place.

Sharelock

CONTACT US

www.sharelock.ai | info@sharelock.ai